

Zero Trust Is Not Enough for Backup

Author: Greg Tevis



cobalt IRON[®]

Executive Summary

Many organizations are improving their security posture by taking a zero-trust approach to infrastructure security. The zero-trust model shifts the security perimeter from the traditional network or organizational boundary down to individual resources and accesses. This approach requires that every access request to every resource be authenticated every time. Once authenticated, users and devices are authorized and continuously validated in order to get or keep access. But there is an inherent flaw in the zero-trust authentication approach: Once authentication is made to the individual resource, access is still permitted! There's no

doubt that a zero-trust mindset is an important improvement to infrastructure and data security, but there is an even better way to protect your critical backup environment.

This paper explores the complexity of the typical backup environment and the challenges associated with the zero-trust model, along with examples. You will learn the fundamentals of Zero Access[®], a new security approach to backup that is better than zero trust, and you will also find out how to identify possible vulnerabilities in your organization's backup landscape and how a Zero Access solution can eliminate them.



Modern Security Concerns... Industry experts are seeing a massive increase in all cyber activity, which generally starts with attempts to obtain credentials, gain access, and exfiltrate or alter data. These heinous activities often end with a final, catastrophic act — such as ransomware — that blows up all or part of the business and forces you to have to recover and maybe pay data ransom demands.

To make matters worse, more and more attackers are adopting AI to make their attacks easier. For example, phishing is an effective way to gain initial access to a network, but phishing can be less effective if an attacker isn't a native English speaker and therefore misspells common words — a dead giveaway to some would-be victims. GenAI solves that problem because it can simulate an email in the voice of someone we know and trust, like a CEO who writes and speaks publicly. Suddenly, we're getting emails from our CEO asking us to buy gift cards.

All of this is especially hard on backup operations.

Sophos' 2024 State of Ransomware report says that 94% of cyber attacks also attempted to compromise backup. That statistic illustrates what a tremendous threat there is against backup environments. For example, there are ransomware

94% *of cyber attacks also attempted to compromise backup.*

— Sophos' 2024 State of Ransomware report

suffered an attack that basically froze large portions of the company's IT, including its backup systems.

Clearly, securing the backup environment is a challenge for enterprises. The zero-trust approach plays an important role, but it's not foolproof, and it's not enough to effectively secure backups.

gangs that specifically target backup environments, and there's a LockBit variant that does the same. UnitedHealthcare, whose CEO says the company repels an attack every 70 seconds, recently

The Good Old Days Are Gone

It used to be that you could build a firewall and other security controls around your network or IT facility, and once credentialed users made it past those controls, they were considered safe, and you could trust them to do anything. If a user was verified once, he or she could move from one resource or set of data to another inside the perimeter without being verified again. There was no reason not to trust those credentials.

Those days are gone. With the addition of cloud; the advent of the mobile workforce; the federation of responsibilities, data, and access; and the distribution of everything, you can no longer build a digital or physical wall around your company. And you can't simply verify credentials once and then trust those credentials forever. It's too easy for attackers to take over user sign-ins, gain access, and move through the organization. As a result, the access controls that worked 10 years ago can't be trusted today.

The Essence of Zero Trust

That's where zero trust comes in. Zero trust is about isolating and authenticating every access to every resource every time. It's no longer "Trust but verify." Instead, it's "Never trust. Always verify."

It's not reasonable to expect that we can stop every attack forever. As long as there are new security tools, practices, and technology, there will be new exploits and vulnerabilities. Fundamentally, zero trust is about preventing attacks as much as possible and reducing the impact of an attack when it happens. By requiring authentication and authorization at every



access point, zero trust brings containment to your security exposures and helps keep problems from spreading.

For that reason, zero trust should most certainly be part of every IT and data protection strategy.

The Complexity and Security Posture of a Typical Backup Environment

But the backup environment is special.

To start with, backup is a unique application in that it is usually the largest application in the enterprise, and it typically contains copies of all the data from all other applications! This makes it a critical resource and a desirable target for deplorable cyber attacks.

In addition, there are many moving parts to even the smallest backup environment. When you get into mid to large size companies and enterprises, the number of software and hardware components and the interactions between them is mind-boggling. And all of those components typically require access. Given that complexity, many, many vulnerabilities still exist, even in the most security-hardened backup operations that deploy zero-trust methods such as multifactor authentication wherever possible.

Despite doing all the right things, some companies have nevertheless fallen prey to cyber criminals. For example, a large company with well-hardened IT operations run by an experienced managed service provider still lost its backup catalog as part of a cyber attack and couldn't recover its data. This is indicative of the complexities of the backup environment and how difficult it is to secure it. Many backup products were not designed for this cyber crime era.

If these disastrous consequences can hit organizations that have prepared well, imagine what can happen to the ones that haven't. While more and more companies are aware of the need for preparation, security hardening, and recovery testing, there are still plenty of companies that fail to test their disaster recovery and other recovery scenarios, including cyber attack scenarios. This failure just compounds an already tough problem and increases the risk to the backup data and business operations.

Why Zero Trust Is Not Sufficient for Securing Backup

Backup must be part of any cyber protection discussion because it is the final safety net for recovery, and zero trust is currently the recommended approach for securing your environment. Zero trust has been touted as the ultimate defense mechanism against data breaches, and it is indeed crucial for improving cyber protection. But when it comes to backup and recovery, you need to think of improving your security posture beyond what you can do with zero trust.

Make no mistake. Everyone should be implementing the zero-trust methodology as applicable. But zero trust has some fundamental shortcomings that make it not well-suited to backup.

Zero trust still results in access — The fundamental challenge with zero trust is that even though it makes access more difficult, the goal is still access. And when there's access, there's potential for harm, especially if the credentials have been stolen. If there's one part of your business that absolutely cannot fall into the wrong hands, it's backup. Yet that possibility is all too real if you're relying on zero trust alone.

Many components means many cyber vulnerabilities — Remember all those moving parts we discussed in the backup environment? Each one is a potential opening for attacks. And security is typically managed separately for each component.

Not all vendors offer zero trust — Not every technology vendor adopts the zero-trust philosophy in how they design, deliver, produce, manage, document, etc. their systems and solutions. And even the backup vendors that do provide advanced security features typically can only do so for their own products, not for the many other components and products that make up a backup environment.



Flaws in the framework — Legacy code and architectures sometimes contain hidden cyber vulnerabilities. One example is the Secure Shell (SSH) protocol and its most common implementation, OpenSSH. This protocol was designed almost 30 years ago as a secure replacement for Telnet and other remote login protocols and was widely used as a management interface option for legacy backup products. Unfortunately, this interface remains in some backup products as a backdoor entry that has been all but forgotten except by cyber criminals. Recent attacks have focused on these vulnerabilities.

Log4j is another great example. Log4j is very commonly used software found in many computer systems, including backup servers, for monitoring and logging events. A specialized cyber attack named Log4Shell exploits openings in this software. It has been many months since this attack emerged, but that doesn't mean that every vendor has produced new software that removes the Log4j vulnerability, nor does every organization apply recommended security patches.

A zero-trust strategy doesn't close backdoors or other vulnerabilities if they are not recognized.

Zero-trust protection doesn't equal cyber resilience

Originally, data backup and recovery were meant to counter hardware failure and human error, not to recover from a security incident. Only recently did cyber crime become a consideration. When hackers strike, backup is sometimes the only thing standing between recovery and ruin. Therefore, the backup environment must now be cyber resilient, meaning that it must withstand attacks and remain intact when any or all other resources have been compromised.

Cyber resilience requires data protection techniques that proactively guard not just against hardware or human failure, but against purposeful bad actors who do things like steal credentials and impersonate trusted entities. Zero trust helps, but it has limitations. Cyber resilience requires a backup system with different, more advanced capabilities than

traditional backup and recovery solutions. The data protection tools you choose must be designed for cyber resilience to be effective against attacks.

Fortunately, there's a way to overcome zero trust's limitations.

A Better Way: Cobalt Iron Compass and the Zero Access Model

For backup, there's a better approach than zero trust. It's called Zero Access®, and it's only available in the Cobalt Iron enterprise SaaS backup platform, Compass. Zero Access helps ensure that in an emergency, your ultimate recovery tool — your backup data — will be safe. Compass and its Zero Access architecture were designed for cyber resiliency in the age of cyber crime. The technology is fundamentally different from traditional backup, recovery, and security methods for data protection.

Automation over access

Many data breaches are caused by attacks that involve human error. That's a perfect example of why Zero Access was invented. The more you can remove human access to the backup environment, the better protected your data will be from human error and human maliciousness.

Compass favors automation over access. In other words, automation eliminates unnecessary human interaction — and thus, human error or malintent — with backup componentry and operations. In doing so, it makes things more secure while also making systems faster, more efficient, and more effective.

Filling gaps in the zero-trust approach

Backup infrastructures have many components, including the backup server and operating system, backup server software, a backup catalog database, reporting tools, a network, and backup storage. Even when those components are protected by zero-trust methods, they still require and allow access.



Compass is optimized to fill the gaps that zero trust leaves behind, eliminating all the normal access points into the entire backup environment for any operational activity and replacing them with automation.

Removing the ability to manage the backup environment manually means it is no longer a target for attack. No one can take over an account, log in to a backup component product, and start destroying things because those logins simply don't exist.

Managing backup through Compass Commander

If there's no access to the backup environment, then you might wonder how anyone can configure and monitor the backups. That's the purpose of Compass Commander, a visibility and management interface for watching the processes, modifying policies, getting reports, etc. While Compass uses Zero Access for delivering the backup infrastructure, it uses zero-trust mechanisms — including multifactor authentication — to control access to the Compass Commander experience. But even full access into the Commander interface does not give access into the backup infrastructure.

“Break glass” procedures and defensible data deletion

Occasionally, there's reason to delete a full backup, such as for a system decommission or when a data deletion or retention policy changes. For those cases, Compass has “break glass” procedures and an Authorization Framework that implement what Cobalt Iron calls defensible data deletion. That's the notion that even administrators cannot delete their own data. There must be an auditable, multifactor approval process. An administrator can have rights to do it, but someone else must approve that deletion because it is a change in data retention controls.

Compass has other break glass procedures as well. For instance, there's a process for gaining access to Compass devices in an emergency. Rarely implemented, this procedure

requires three-phase security approval on the Cobalt Iron side combined with the customer side.

Those break glass procedures and the Authorization Framework are an important part of the Compass security design and help to reinforce the Zero Access approach.

Other Cyber Resilient Features in Compass

Besides Zero Access, Compass has additional security features that make it the ultimate backup platform for cyber resiliency, such as ...

- **Ransomware monitoring and detection for dozens of data distortion patterns.**
- **Ransomware analytics including impact analysis, cyber event insights, and recommended recovery points and objects.**
- **Backup data immutability.**
- **Multiple, isolated security zones as part of backup processes.**
- **Virtual air-gapped backup data.**
- **Multiple layers of encryption to prevent possibility of data exfiltration.**
- **Data validation and security on ingest and access.**
- **Data life cycle governance.**
- **An Audit Framework to track all operational metrics and activities.**

Think of Compass as a hardened-as-a-service product. As part of the Compass enterprise, private SaaS backup platform, you get Zero Access automation that takes backup out of the equation when hackers go looking for places to attack.



A Zero Access Success Story: One Compass Customer's Experience

A global company that relies on Cobalt Iron Compass was hit with a massive ransomware attack on its production Windows environment. Hackers used stolen credentials to get into the company's production Active Directory and compromise more than 1,000 systems. Because of Zero Access, backups were completely protected, and the customer recovered while never communicating with the cyber criminals.

A second wave occurred a couple of weeks later that inflicted further damage. Again, the company recovered thanks to Compass. After failing to collect a ransom, the attackers had actually threatened to go after the company's backup, but instead, they were never heard from again. Because of Compass' Zero Access architecture, the dozens of vulnerable access points that plague a typical backup environment — vulnerabilities these hackers had depended on when they made their threat — simply don't exist in Compass to be attacked.

As this customer discovered, Compass offers a higher level of comfort that backups are protected, not just with zero trust but with Zero Access architecture and methodology.

The following [Backup Environment Security Vulnerability Questionnaire](#) will help you start thinking through your backup environment and determine if the Compass Zero Access approach makes sense for your circumstances. As you go through your backup security review, feel free to reach out to Cobalt Iron to discuss.



Identify Security Vulnerabilities in Your Backup Environment and Discover How Zero Access Can Help

When disaster strikes, a properly protected, cyber resilient backup environment can mean the difference between restoring the business and going under. So it pays to review your backup security posture and put cyber resilient backup capabilities in place.

888-584-4766 • www.cobaltiron.com

cobalt IRON®

© 2026 Cobalt Iron, Inc. All rights reserved. Cobalt Iron, the Cobalt Iron logo, Compass, and the Compass logo are registered trademarks; and the Cobalt Iron agent logo, "Data Protection Everywhere. Smart. Secure. Automated.", and Take Control of Your Data are trademarks of Cobalt Iron. All other trademarks or registered trademarks are the property of their respective owners. 100120